

**RAÚL TORREZ, Attorney General**

P. Cholla Khoury  
Jacqueline N. Ortiz  
Judy Paquin  
Assistant Attorneys General  
P.O. Drawer 1508  
Santa Fe, NM 87504  
Tel: (505) 490-4060  
[ckhoury@nmag.gov](mailto:ckhoury@nmag.gov)  
[jortiz@nmag.gov](mailto:jortiz@nmag.gov)

David M. Berger (SBN 277526)

**GIBBS LAW GROUP LLP**

1111 Broadway, Suite 2100  
Oakland, California 94607  
Telephone: (510) 350-9700  
Facsimile: (510) 350-9701  
[dmb@classlawgroup.com](mailto:dmb@classlawgroup.com)

*Attorneys for Proposed Plaintiff-Intervenor  
State of New Mexico*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION**

IN RE: FACEBOOK, INC. CONSUMER  
PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

**DICELLO LEVITT LLC**

Adam J. Levitt  
Amy E. Keller  
Ten North Dearborn St., Sixth Floor  
Chicago, IL 60602  
Tel.: (31) 214-7900  
[alevitt@dicellolevitt.com](mailto:alevitt@dicellolevitt.com)  
[akeller@dicellolevitt.com](mailto:akeller@dicellolevitt.com)

Corban Rhodes (pro hac vice forthcoming)  
485 Lexington Avenue, Suite 1001  
New York, NY 10017  
Tel.: (646) 933-1000  
[crhodes@dicellolevitt.com](mailto:crhodes@dicellolevitt.com)

Case No. 3:18-MD-02843-VC

**DECLARATION OF CORBAN S. RHODES  
IN SUPPORT OF THE STATE OF NEW MEXICO'S MOTION TO INTERVENE**

1 I, Corban S. Rhodes, declare as follows:

2 1. I am counsel by special commission to the Attorney General of New Mexico in the action  
3 titled *State of New Mexico ex rel. Raúl Torrez v. Facebook, Inc.*, No. D-101-cv-2021-00132  
4 (Santa Fe Cty.) (the “New Mexico Action”).

5 2. The State filed its Complaint in the New Mexico Action on January 21, 2021. A true and  
6 correct copy of the Complaint is attached hereto as Exhibit A.

7 3. On January 13, 2023, my firm sent a letter on behalf of the NMAG to counsel from  
8 Gibson Dunn representing Meta, Inc. in both the New Mexico Action and the above-captioned  
9 action, *In re Facebook, Inc. Consumer Privacy User Profile Litigation*, 18-md-02843-VC  
10 (N.D.Cal.) (the “MDL Action”), Mr. Russ Falconer. A true and correct copy of the letter is  
11 attached hereto as Exhibit B.

12 4. The purpose of the letter was to confirm the State’s understanding that the Settlement  
13 Agreement does not release any of the State’s claims, and that Meta will not raise any arguments  
14 in any future proceeding to the contrary. The letter requested a response from Meta no later than  
15 January 20, 2023, and explained that if the State did not receive such confirmation, the State  
16 would need to “intervene and/or object in the MDL proceedings, in order to protect and preserve  
17 the claims asserted in the State’s Action.” As stated in that letter, the State had not received any  
18 notification pursuant to the Northern District of California’s Procedural Guidance for Class  
19 Action Settlements, and continued to receive no such notice until, arguably, today, as described  
20 below.

21 5. Having heard no response from Meta, on Saturday, February 4, 2023, I spoke with Mr.  
22 Falconer by phone, and asked when Meta intended to respond to the January 13 letter, and he told  
23 me that he did not have an update but would speak with his client about it.

24 6. On February 16, 2023, I followed up with Mr. Falconer by email and asked that Meta  
25 respond to the State’s letter no later than February 24, 2023. Mr. Falconer responded the  
26 following day, February 17, 2023 that Meta was “actively working on our response to your  
27 letter,” but we received no response by February 24, 2023.  
28

1 7. On February 27, 2023, I followed up with Mr. Falconer again by email and explained that  
2 if Meta did not confirm, in writing, that it will not take the position that New Mexico's claims are  
3 released or otherwise impacted by the MDL Settlement Agreement by 5 p.m. EST on February  
4 28, 2023, that the State intended to file a motion to intervene in the MDL Action.

5 8. On the morning of February 28, 2023, Mr. Falconer sent an email containing Meta's  
6 response to our January 13, 2023 letter. A true and correct copy of that email is attached hereto  
7 as Exhibit C.

8 9. I subsequently spoke with Mr. Falconer by phone shortly after receiving his February 28  
9 email and notified him that the State would likely proceed with a motion to intervene and seek to  
10 be heard at the preliminary approval hearing scheduled for March 2, 2023.

11 10. As detailed above, the State has made every reasonable effort to notify Meta's counsel,  
12 repeatedly and at the earliest possible time, of the State's intent to intervene in the MDL Action in  
13 order to ensure that its claims are not extinguished via the Settlement Agreement. The State has  
14 therefore complied with the requirements set forth in the Court's Standing Order for Civil Cases  
15 to bring this application on an expedited basis so that the Court may be made aware of issues that  
16 pertain to the preliminary approval hearing set for March 2, 2023.

17  
18  
19 I declare under penalty of perjury that the foregoing is true and correct.

20 Dated: February 28, 2023

21  
22  
23  
24  
25  
26  
27  
28  


---

Corban S. Rhodes

# EXHIBIT A

FILED 1st JUDICIAL DISTRICT COURT  
Santa Fe County  
1/21/2021 9:01 AM  
KATHLEEN VIGIL CLERK OF THE COURT  
Marquel Gonzales-Aragon

**STATE OF NEW MEXICO  
COUNTY OF SANTA FE  
FIRST JUDICIAL DISTRICT**

STATE OF NEW MEXICO, *ex rel.* HECTOR  
BALDERAS, Attorney General,

Plaintiff,

v.

FACEBOOK, INC.,

Defendant.

No. D-101-CV-2021-00132

JURY TRIAL DEMANDED

Case assigned to Mathew, Francis J.

**COMPLAINT**

COMES NOW Plaintiff, the State of New Mexico, by the Honorable Hector H. Balderas, Attorney General of the State of New Mexico (“Plaintiff” or “New Mexico” or the “State”), and brings this action against Defendant Facebook, Inc. (“Facebook”), seeking statutory penalties and all damages, recoverable at law or in equity, to remedy Facebook’s violations of the State’s Unfair Practices Act, NMSA 1978, Section 57-12-1 to -26 (1967, as amended through 2019) (“UPA”). In support of its Complaint, the State avers as follows:

**I. INTRODUCTION**

1. Consumers believe that online privacy is important—so much so that nearly half of consumers surveyed recently believed that privacy is more important than national security.<sup>1</sup> The proliferation of social media and social networking websites creates myriad privacy and security

---

<sup>1</sup> 45 Percent of Americans Think Online Privacy Is More Important Than National Security (Jan. 28, 2015), <https://www.prnewswire.com/news-releases/45-percent-of-americans-think-online-privacy-is-more-important-than-national-security-300026808.html>.

concerns—allowing those with access to profiles to see contact information, photos, and even geolocations.<sup>2</sup>

2. Consumers have placed a great deal of trust in providers of social media services to keep certain information private based upon the explicit representations those providers make. Consumers’ trust in a provider is even more important when that provider—like Facebook—forces consumers to identify themselves, eliminating anonymity on the web.<sup>3</sup>

3. Facebook’s cultivation of user trust—through explicit representations that it protected user information and ensured that unauthorized users would not be able to see private information—led to nearly 79 percent of consumers in 2017 agreeing that Facebook had a commitment to protecting user privacy.<sup>4</sup>

4. But Facebook’s cultivation of consumer trust was a charade. Facebook’s failure to abide by its promises to consumers was revealed, in part, when the personal information of 70 million Americans, including nearly 350,000 New Mexico residents, was exposed to unauthorized third parties in the highly-publicized Cambridge Analytica scandal.<sup>5</sup>

---

<sup>2</sup> Alice Karanja, Daniel W. Engels, Ghizlane Zerouali, Ariel Francisco, *Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media*, SMU Data Sci. Rev. Vol. 1, No. 2, Art. 13 (2018), available at <https://scholar.smu.edu/cgi/viewcontent.cgi?article=1042&context=datasciencereview>.

<sup>3</sup> Maggie Tillman, *10 Reasons why Facebook has thrived for 15 years*, Pocket-lint (Feb. 4, 2019), <https://www.pocket-lint.com/apps/news/facebook/126998-10-reasons-why-facebook-has-lived>.

<sup>4</sup> Herb Weisbaum, *Trust in Facebook has dropped by 66 percent since the Cambridge Analytica Scandal*, NBC News (Apr. 18, 2018), <https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011>.

<sup>5</sup> See Prachi Bhardwaj and Samantha Lee, *Here’s a state-by-state breakdown of Facebook users impacted by the Cambridge Analytica scandal*, Business Insider (June 16, 2018), available at <https://www.businessinsider.com/facebook-cambridge-analytica-affected-us-states-graphic-2018-6>; State-by-State Breakdown of People Whose Facebook Information May Have Been Improperly Shared with Cambridge Analytica, <https://about.fb.com/wp-content/uploads/2018/05/state-by-state-breakdown.pdf> (last accessed Dec. 21, 2020).

5. While Mark Zuckerberg, Facebook’s CEO, acknowledged that Facebook’s conduct in relation to the Cambridge Analytica scandal was a “major violation of people’s trust” and that Facebook “didn’t do enough” to protect Facebook users’ personal data, the Cambridge Analytica scandal is only one of many instances where Facebook enabled unauthorized third parties to access and use consumers’ private information without their knowledge or consent—while, at the same time, representing to consumers that its privacy policies did not permit such access and use.

6. Indeed, Facebook’s deceptive data practices pervade its entire business model. As one researcher put it:

It was standard practice and encouraged. Facebook was literally racing towards building tools that opened their users’ data to marketing partners and new business verticals. So this is something that’s inherent to the culture and design of the company.”<sup>6</sup>

In other words, Facebook has a practice of enabling third parties to access and use consumers’ personal information, despite telling consumers that they could control the security of their own personal data.

7. Facebook’s dismissive and cavalier attitude toward user privacy is not new. Rather, it has been consistently aggressive since its founding, as reflected in early emails and IMs, such as the following exchange between 19-year-old Mark Zuckerberg and a friend shortly after Zuckerberg launched The Facebook in his dorm room:

**Zuck:** Yeah so if you ever need info about anyone at Harvard

**Zuck:** Just ask.

**Zuck:** I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How’d you manage that one?

---

<sup>6</sup> Julia Carrie Wong, Mark Zuckerberg apologises for Facebook’s ‘mistakes’ over Cambridge Analytica (Mar. 22, 2018), available at <https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica>.

**Zuck:** People just submitted it.

**Zuck:** I don't know why.

**Zuck:** They “trust me”

**Zuck:** Dumb f\*\*\*s.<sup>7</sup>

8. Facebook’s disregard for consumer privacy is further compounded by the algorithms that it uses; some of the same information which Facebooks represents to users will be kept private is used to target users with an endless stream of information that Facebook believes consumers will “like,” without regard to its truthfulness or accuracy.

9. Facebook operates the world’s largest social media platform, with 2.45 billion users and annual revenue of \$ 70.7 billion in 2019—99.9% of which comes from advertising.<sup>8</sup> It allows people and organizations to create personalized online profile pages about themselves, filled with biographical details, photos, and a scrollable “news feed” or “wall” of chronological “posts,” either about the user or posted by the user.

10. Facebook also lets users connect with other users as “friends,” and promises its users that they have the ability to restrict access to their information using various privacy settings.

11. Facebook also promised consumers via its Terms of Service and Data Policy that third-party applications and their developers were required to respect all Facebook consumers’ privacy, and stated in its Platform Policy that it had the ability to audit third-party applications and take enforcement measures against those applications.

---

<sup>7</sup> Nicholas Carlson, *Well, These New Zuckerberg IMs Won’t Help Facebook’s Privacy Problems*, Business Insider (May 13, 2010), <https://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5?IR=T>.

<sup>8</sup> Business of Apps, Facebook Revenue and Usage Statistics <https://www.businessofapps.com/data/facebook-statistics/> (last updated Oct. 30, 2020).



12. New Mexico consumers expected that Facebook would abide by its privacy policies, and prevent third-party application developers from seeing, using, and profiting from their private information. Despite Facebook's promises regarding privacy, it did not follow its own policies, nor did it prevent third parties from seeing users' private information.

13. Hundreds of thousands of consumers in the State of New Mexico use Facebook's social networking website and its companion mobile device application.

14. Facebook accumulates, stores, and maintains a collection of its consumers' personal data, including New Mexico consumers, as well as data regarding their digital behavior both on and off the various Facebook platforms. Some, including New Mexico Senator, Ben Ray Lujan, have even expressed concern about Facebook's alleged collection and accumulation of the personal data of even those consumers who do not use Facebook. As Senator Lujan stated, despite Facebook's false and misleading assertion that "everyone controls their own data," Facebook is "collecting data on people that are not even Facebook users, that have never signed a consent or privacy agreement."<sup>9</sup>

15. Facebook's consumers reasonably rely on Facebook to take appropriate steps to maintain and protect their data. Even though Facebook informs its consumers of the safety measures it takes, promising that it requires applications to respect all Facebook consumers' privacy, in reality, Facebook has failed to follow-through and fulfill this promise, and outright lied about its consumers in the process.

---

<sup>9</sup> Zuckerberg Faces Intense Questioning Before House Panel, Courthouse News Service (Apr. 11, 2018), available at <https://lujan.house.gov/media-center/press-releases/zuckerberg-faces-intense-questioning-before-house-panel>.

16. Facebook grants third-party developers—including developers of applications and mobile device makers—access to its users’ sensitive information in connection with their offering applications to Facebook users.

17. In 2007, Facebook launched a developer portal that allowed third-party software developers to create applications that interacted with Facebook users. These “Facebook apps,” like applications on a mobile phone, are programs that operate on Facebook’s website or mobile application. Facebook apps include games and quizzes.

18. The Facebook apps were not only able to access publicly-available data about its users, but also non-public data—information that users thought they had restricted—about both themselves and their friends.

19. This practice was deceptive, and in 2011, Facebook and the Federal Trade Commission entered into a consent decree mandating that Facebook “not misrepresent any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to: . . . (C) the extent to which [Facebook] makes or has made covered information accessible to third parties.” *In the Matter of Facebook, Inc.*, No. 092 3184, Agreement Containing Consent Order, at Section I.C. (“FTC Consent Order”). The FTC Consent Order includes several other provisions imposing minimum security and disclosure requirements on Facebook to its users.<sup>10</sup>

20. Despite this consent decree, and despite representing to users that the company had safeguards in place to protect their data, Facebook allowed third parties to access data that Facebook users thought that they had restricted.

---

<sup>10</sup> References made to the FTC Consent Order are for reference only and are not made in order to allege an independent federal cause of action or any substantial federal question. The State brings this action exclusively under the laws of the State of New Mexico.

21. Facebook lacks adequate enforcement and supervision of privacy restrictions on third-party applications, as is demonstrated here. For example, from 2013-2015, Facebook permitted Cambridge University researcher Aleksandr Kogan (“Kogan”) to use a third-party application created in conjunction with his company Global Science Research (“GSR”) to harvest the personal data of approximately 70 million Facebook consumers in the United States, including approximately 350,000 consumers in New Mexico, then sell it to Cambridge Analytica, a political consulting firm that used this Facebook data to target voters and influence the 2016 United States General Election, as well as other elections throughout the world. Kogan’s application was installed by thousands of distinct Facebook consumers in New Mexico, but the application also collected the personal information of users’ Facebook friends—including hundreds of thousands of New Mexico residents—who did not consent to the collection of their data. The number of detrimentally affected Facebook friends is significant, as these users did not download Kogan’s application and, therefore, were not notified of the privacy implications and problems that would arise from another Facebook friend downloading and using the Kogan application.

22. Cambridge Analytica is not the only example. Other entities include Global Science Research Ltd., SCL Group Limited, SCL Elections Ltd., and SCL USA Inc., which all participated in unlawfully obtaining and retaining the full names, telephone numbers, mailing addresses, email addresses, ages, interests, physical locations, political and religious affiliations, relationships, pages liked, and social groups of approximately 87 million Facebook users.

23. Importantly, this profound access to personal information only tells part of the story. The consequences of Facebook’s actions are dire—not only has the private information of

consumers been exposed, but, because of Facebook’s continued failure to follow its own policies, consumers are targeted with “sustained and ongoing”<sup>11</sup> sophisticated disinformation campaigns.

24. Facebook likes, comments, and shares of articles from news outlets that regularly publish provably false content and misleading, unsubstantiated claims roughly tripled from the third quarter of 2016 to the third quarter of 2020.<sup>12</sup> The growth rate of likes, shares, and comments of content from manipulators and false content producers exceeded the interactions that users had with legitimate journalistic outlets such as Reuters, Associated Press, and Bloomberg.<sup>13</sup>

25. Facebook relies upon viral content to bring in its users. As a result, although Facebook *can* address these issues if it desires, it has little incentive to do so, because it would impact Facebook’s bottom line. In sum: Facebook does well when it allows misinformation to spread.

26. There is no greater example of the dangers of Facebook’s incentivization and rewarding of exaggerations and lies than the siege on the U.S. Capitol on January 6, 2021. Facebook’s misuse of its users’ data has enabled those wishing to do so to target and share more extreme views on the platform directly with an audience that Facebook’s own data trove indicates will be receptive—rewarding these actors with the ability to accumulate likes and shares for posts on subjects like election fraud conspiracies, SARS-CoV-2 or “Coronavirus” denialism, and anti-

---

<sup>11</sup> Natasha Korecki, ‘Sustained and ongoing’ disinformation assault targets Dem presidential candidates, Politico (Feb. 20, 2019), <https://www.politico.com/story/2019/02/20/2020-candidates-social-media-attack-1176018>; Sandeep Gopalan, *Hate speech, fake news, privacy violations—time to rein in social media*, The Hill (Nov. 16, 2018), <https://thehill.com/opinion/technology/417049-hate-speech-fake-news-privacy-violations-time-to-rein-in-social-media>.

<sup>12</sup> Davey Alba, *On Facebook, Misinformation Is More Popular Now Than in 2016*, The New York Times (Oct. 12, 2020), <https://www.nytimes.com/2020/10/12/technology/on-facebook-misinformation-is-more-popular-now-than-in-2016.html>.

<sup>13</sup> *Id.*

vaccination rhetoric.<sup>14</sup> Because of Facebook’s surreptitious use of user information, Facebook users with unremarkable feeds can transform into “influencers” seemingly overnight for sharing misinformation.<sup>15</sup> New Mexico consumers are exposed to this misinformation based upon Facebook’s algorithms. As a result, influencers are rewarded with surging likes and shares, more followers, and enhanced reputations, while simultaneously creating an alternate false reality based on misinformation in an ecosystem charged by hyper-partisan politics. Influencers’ impact is even more outsized in Facebook groups created by and for like-minded people, echo chambers where misinformation snowballs and disparate conspiracy factions can unite into a larger movement—a kind of mass radicalization.<sup>16</sup>

27. The misinformation is, unfortunately, spread in a not insignificant part by elected officials. For example, researchers at Cornell University recently found that President Donald Trump was the “single largest driver” of Coronavirus misinformation.<sup>17</sup> Concerning the November 2020 election, the Facebook pages that spread the most misinformation belonged to Mr. Trump, his son, and right-wing commentators.<sup>18</sup> Despite this common knowledge, Facebook has long declined to interfere with Mr. Trump’s posts, which have often been filled with falsehoods

---

<sup>14</sup> Stuart A. Thompson and Charlie Warzel, *They Used to Post Selfies. Now They’re Trying to Reverse the Election: Right-wing influencers embraced extremist views, and Facebook rewarded them*, The New York Times (Jan. 14, 2021), <https://www.nytimes.com/2021/01/14/opinion/facebook-far-right.html?referringSource=articleShare>.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> Sheryl Gay Stolberg and Noah Weiland, *Study Finds “Single Largest Driver” of Coronavirus Misinformation: Trump*, New York Times (Oct. 22, 2020), <https://www.nytimes.com/2020/09/30/us/politics/trump-coronavirus-misinformation.html>.

<sup>18</sup> Ben Gilbert, *The Facebook pages that spread the most election misinformation belong to Trump, his son, and a set of right-wing commentators, new research finds*, Business Insider (Nov. 24, 2020), <https://www.businessinsider.com/trumps-conservative-pundits-responsible-election-misinformation-avaaz-2020-11>.

and threats yet were published largely unimpeded.<sup>19</sup> With more than 35 million followers, Mr. Trump's Facebook posts and their comment sections were a lightning rod for influencers seeking fans.<sup>20</sup> The effect: Facebook has become an incubator for insurrection, and a threat to democracy itself.

28. This threat to democracy became clear on the morning of January 6, 2021—the day when Congress first began counting electoral votes to certify President-Elect Joseph R. Biden's victory in the November 2020 presidential election. Congress' work was violently interrupted by an insurrection at the nation's capital. Although Facebook has largely downplayed its role in the insurrection, there is no doubt that radical, white supremacist movements and groups have been able to grow on platforms like Facebook to spread conspiracy theories, incite violence, coordinate illicit activities, and feed conspiracy theorists' thirst for misinformation.<sup>21</sup>

29. The State brings this lawsuit because Facebook repeatedly breached and violated its promises that it would restrict access to consumers' private data in accordance with the consumers' privacy settings, all while allowing misinformation grow through this access to private data. Rather than honor its promises, Facebook knowingly enabled application developers and

---

<sup>19</sup> Mike Isaac and Kate Conger, *Facebook Bars Trump Through End of His Term*, The New York Times (published Jan. 7, 2021, updated Jan. 8, 2021), <https://www.nytimes.com/2021/01/07/technology/facebook-trump-ban.html>. Facebook acknowledges as much: “Over the last several years, we have allowed President Trump to use our platform consistent with our own rules, at times removing content or labeling his posts when they violate our policies.” Guy Rosen and Monika Bickert, *Facebook: Our Response to the Violence in Washington*, Facebook (Jan. 6, 2021), <https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/>.

<sup>20</sup> Stuart A. Thompson and Charlie Warzel, *They Used to Post Selfies. Now They're Trying to Reverse the Election: Right-wing influencers embraced extremist views, and Facebook rewarded them*, The New York Times (Jan. 14, 2021), <https://www.nytimes.com/2021/01/14/opinion/facebook-far-right.html?referringSource=articleShare>.

<sup>21</sup> Rebecca Heilweil and Shirin Ghaffary, *How Trump's Internet build and broadcast the Capitol insurrection*, Vox (Jan. 8, 2021), <https://www.vox.com/recode/22221285/trump-online-capitol-riot-far-right-parler-twitter-facebook>.

other third parties to do an end-run around consumers' privacy settings by granting them access to user data, even if those users restricted it. Consumers placed trust in Facebook to keep their information secure. Instead, Facebook allowed unauthorized parties to access that information, and use it to spread false and misleading information back to Facebook's users. Facebook's flouting of its own privacy policies has contributed to the spread of misinformation, viral propaganda, and hate campaigns worldwide. The State brings this lawsuit for the safety, general health and welfare of the people of New Mexico, and to hold Facebook accountable for its actions.

30. Facebook ignored its duties to its consumers and disregarded its obligations to the federal government when it did not take the fundamental step of reviewing the third-party application it allowed to run on its site. Reading Kogan's application's terms would have easily alerted Facebook of Kogan's intention to improperly sell consumer data, further demonstrating the inadequate oversight of third-party applications.

31. Once Facebook discovered Kogan's improper sale of consumer data to Cambridge Analytica, it failed to take reasonable and responsible steps to protect its consumers' privacy. Facebook could have, but did not, attempt to have all stolen data returned and/or deleted by Kogan and Cambridge Analytica.

32. Facebook then neglected to timely notify the public (including New Mexico residents) that Cambridge Analytica, an unknown third-party, purchased tens of millions of Facebook's consumers' data, even though Facebook knew, or should have known, that such data was acquired in violation of its policies and was being used in connection with politics generally and election influencing specifically. Instead, Facebook waited until a whistleblower exposed its improper conduct to the public before it responded.

33. By waiting to inform consumers that their information was exposed, purchased, and used without their consent, Facebook was able to profit when Cambridge Analytica used the underlying purchased information to purchase targeted advertising on Facebook to the very individuals whose data it purchased.

34. Facebook violated the State's UPA by its actions alleged herein regarding its policies and business practices pertaining to third-party application access to and use of Facebook consumers' data. Specifically, (1) Facebook misrepresented its policies for protecting its consumers' personal data, especially with regard to permissions it granted to third-party applications when allowing them access to consumers' personal information for their own use, subject to the consumer agreement's terms; (2) Facebook failed to inform its consumers that their data was accessible by third-party applications downloaded by their friends on Facebook without their affirmative consent or knowledge; (3) Facebook did not inform impacted consumers when their data was wrongfully harvested and used by third-party applications in violation of Facebook's security and privacy policies, as demonstrated by Kogan's application and sale of private consumer data to Cambridge Analytica; (4) Facebook's privacy settings are unclear, ambiguous, and incomprehensible, in addition to their false representations and inadequate disclosures to consumers regarding the security of their data; (5) Facebook failed to disclose that it permitted many mobile device-making companies and specific other companies access to consumer data, including permission to alter consumer privacy settings.

35. Facebook could have and should have prevented third parties from misusing its consumers' private data. Facebook should have implemented and maintained reasonable oversight of third-party applications consistent with its representations to the public, terms of service, and internal policies. The State brings this action to ensure that Facebook is held accountable for its



failure to protect its consumers' privacy and personal data. The State seeks civil penalties and costs to deter Facebook from engaging in these and similar unlawful trade practices, injunctive relief to prevent Facebook from engaging in these and similar unlawful trade practices, and any appropriate restitution for consumers.

## II. JURISDICTION

36. This Court has personal jurisdiction over Defendant Facebook because, among other things:

- a. Facebook operates a data center within the State,<sup>22</sup> conducts business within the State, and has registered with the New Mexico Secretary of State to do business within the State in accordance with the New Mexico Business Corporation Act, NMSA 1978, Sections 53-17-1 to -20 (2013). *See Rodriguez v. Ford Motor Co.*, 2019-NMCA-023, ¶¶ 24-28, 458 P.3d 569, 580-82 (finding foreign corporation consented to personal jurisdiction in New Mexico by registering under the Business Corporation Act).
- b. Facebook willfully placed its Facebook website and Facebook application for mobile devices into the stream of commerce with the knowledge and intent that its products would be widely disseminated throughout the world, including the United States and the State of New Mexico, and with knowledge that the adverse effects of the inadequate data security would be felt in the State of New Mexico. Facebook also targeted its specific misrepresentations at citizens of the State of New Mexico, when it told them—falsely—that they could control who

---

<sup>22</sup> Davis, Ron, *Facebook's third data center building goes online in Los Lunas*, Albuquerque Business First (June 19, 2020), available at <https://www.bizjournals.com/albuquerque/news/2020/06/19/facebook-third-data-center-building-goes-online.html>

does and does not see their user information. As such, Facebook has established sufficient minimum contacts with New Mexico and jurisdiction is proper. *See generally Sproul v. Rob & Charlies, Inc.*, 2013-NMCA-072, 304 P.3d 18.

37. This Court has jurisdiction over the subject matter of this case pursuant to NMSA 1978, Sections 38-3-1(A) and (F) (1988), NMSA 1978, Section 57-12-8 (1977), and NMSA 1978, Section 57-12-11 (1970).

### **III. VENUE**

38. Venue is proper in Santa Fe County because Plaintiff resides here, and some or all of the acts, practices, and conduct of Facebook, which give rise to this civil action, occurred in Santa Fe County. *See* §§ 38-3-1(A) and (B), 57-12-8.

### **IV. PARTIES**

39. Plaintiff is the State of New Mexico, by the Honorable Hector H. Balderas, the duly-elected Attorney General of the State of New Mexico, who has the statutory authority to enforce laws for the protection of the public. The Attorney General is authorized to act on behalf of the State in all actions when the interests of the State require action in his judgment, and is further empowered to prosecute all actions and proceedings brought by any State officer or head of a State department, board or commission, or any employee of the State in his official capacity. NMSA § 8-5-2(B-C) (1975).

40. The Attorney General is responsible for upholding the public interest and is also specifically authorized to enforce the State's consumer protection laws, including the New Mexico Unfair Practices Act. *See* § 57-12-8.

41. Facebook is a Delaware corporation with its headquarters and principal place of business at 1 Hacker Way, Menlo Park, California 94025. Facebook engages in the business of

supplying social networking services through its website, [www.facebook.com](http://www.facebook.com), and accompanying mobile device applications, to consumers throughout the United States, including in the State of New Mexico.

## **V. FACTUAL ALLEGATIONS**

### **A. Facebook Fails to Protect Collected Consumer Data**

42. Since its creation in 2004, Facebook has continued to grow its user base, amassing billions of consumer users throughout the world, including millions of people in the United States, including in the State of New Mexico. Facebook is among the world's most heavily trafficked websites. Close to one million New Mexico's residents use Facebook's website and/or mobile application.

43. As intended by Facebook, Facebook users build social networks with other users and share information within those networks. To begin using Facebook, a consumer must create a Facebook account, inputting various pieces of personal information such as name, e-mail address, age, gender identity, and more. The consumer can then add other Facebook users as "friends" and has the option to provide additional information, photos, or other content in order to customize their "profile." By accumulating Facebook friends, Facebook's users build social networks on Facebook.

44. Facebook encourages its users to customize their profiles by supplying personal information and "liking" Facebook pages and posts that the users enjoy or agree with.

45. Facebook keeps a personal data file for each consumer, consisting of personal information supplied and metadata created through adding "friends" or "liking" pages, which varies among users.

46. Every Facebook user agrees to abide by the terms of service in exchange for access to the platform as well as the promise that Facebook will secure all of the personal data provided and created through consumers' use of its social media platform.

47. Facebook can determine which consumers wished to keep their information private, and which consumers' information was shared despite making their information private.

48. As Facebook consumers develop their profiles on the platform, they also grow their social networks and interact with friends via the Facebook website. All of this information and activity is digitally collected, recorded, and maintained by Facebook. This data can be divided into two broad categories: (i) data supplied directly by consumers, and (ii) data and metadata created from consumers' activity on and off the Facebook website.

49. Facebook's platform is designed to encourage consumers to continue supplying personal information in the form of "posts," which are shared with that consumers' friends on their respective "timelines," which aggregate the posts made by all friends that are being "followed." posts include, but are not limited to: written statements, photographs and videos, links to websites, and "check-ins" to geographic locations such as restaurants, bars, stores, and other establishments.

50. Facebook also operates a companion mobile application called "Facebook Messenger," which allows Facebook consumers to send and receive private text messages and make phone and video calls via the App. For Facebook Messenger users, Facebook maintains records of messages sent and received and the date and time of phone and video calls made, and the parties to whom all communications are directed. All of this data is stored in one of the largest repositories for data information in the world.

51. Another example of consumer supplied activity data that Facebook collects is a consumer's "likes" or "reactions"—one of Facebook's signature innovations. It allows consumers

to click on a “thumbs-up” icon to like a vast array of online content, or hold down the “thumbs-up” to react to posts with images depicting that a user “loves” a post, thinks a post is funny, is surprised by the post, is saddened by the post, or is angered by the post. Among other things, Facebook consumers can like or react to “posts” made by other Facebook consumers, like “Pages” maintained by non-individual entities, and interact with content on external websites.

52. Facebook’s like and reaction features incentivize increased activity on the Facebook platform by allowing users to reward each other for sharing information—the more posts a consumer makes, the more likely they are to receive more likes or reactions. The “like” and “reaction” functions also serve a broader purpose. Tracking a consumer’s allocation of likes and reactions over time reveals personal information about them—the friends they interact with most, the brands they are drawn to, and the political and social issues they identify with. Facebook’s records each and every one of its consumers’ likes and reactions not only to allow for consumers to engage with one another, but also to give corporate insight into the thought processes of its consumers for advertising purposes.

53. Selling targeted advertising space generates 99.9% of Facebook’s revenue.<sup>23</sup> Facebook relies on its collection and interpretation of each consumer’s data to sell advertising space to marketers looking to target specific individuals and demographics. In exchange for its social networking services, users are required to provide Facebook with their personal data, which Facebook monetizes through the sale of targeted advertising.

54. Despite Facebook’s opportunistic monetization of its users’ personal information and data, Facebook has put data security on the backburner of priorities for almost a decade. According to a former manager-turned-whistleblower at Facebook, he warned executives of the

---

<sup>23</sup> Business of Apps, Facebook Statistics, *supra* n. 8.

companies for years about the dangers of not improving their data protection services starting back in 2011.<sup>24</sup> Even in the face of this warning, Facebook continued to exhibit nonchalance towards data security in March 2019 when it was made public that an internal plain text file containing hundreds of millions of passwords for Facebook, Facebook Lite, and Instagram users was accessible by approximately 20,000 Facebook employees.<sup>25</sup>

55. Facebook was specifically made aware years ago that its platform could be leveraged by third-party applications in order to steal users' personal information. Facebook also knew or should have known that it was not adequately overseeing and monitoring the actions of third-party application developers that were given access to the platform by Facebook. Facebook also knew or should have known that its terms misrepresented the amount of personal information being collected and the level of security implemented for protecting each user's data to its consumers.

56. "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so we had no idea what developers were doing with the data," the aforementioned whistleblower and former manager at Facebook said in 2018.<sup>26</sup> He went on to say that the Cambridge Analytica breach "could have [been] prevented" had executives

---

<sup>24</sup> Shona Ghosh, *Apple has reportedly hired a fierce Facebook critic after repeatedly attacking the firm's 'industrial' data hoarding*, Business Insider (Jan. 13, 2019), available at <https://www.businessinsider.com/apple-has-hired-facebook-critic-sandy-parakilas-the-ft-reports-2019-1>.

<sup>25</sup> Keeping Passwords Secure, Facebook (Mar. 21, 2019), available at <https://about.fb.com/news/2019/03/keeping-passwords-secure/>.

<sup>26</sup> Paul Lewis, *'Utterly horrifying': ex-Facebook insider says covert data harvesting was routine*, The Guardian (Mar. 20, 2018), available at <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>.

heeded his warnings, and opined that in regards to Facebook’s control over data taken by third-party applications, Facebook had “[z]ero. Absolutely none.”<sup>27</sup>

**B. The Facebook Platform and Third-Party Facebook Applications**

57. Facebook launched the Facebook platform in 2007. This system of software (where third-party developers can build applications that interact with the Facebook website) includes various services and tools designed to assist third-party developers to create such applications.

58. Millions of third-party applications have been developed and made available to Facebook consumers using the Facebook platform over the past twelve years or more. Some of these applications are social, such as those that allow consumers to play games against one another. Others are functional, allowing consumers to integrate information from their calendars and email accounts with their Facebook account.

59. The Facebook platform facilitates integration between Facebook and third-party applications. For example, a third-party application developer can allow Facebook consumers to access their application with a service available on the Facebook platform called “Facebook Login.” This application is permitted to carry out its actions via Facebook’s Software Development Kit. Facebook Login allows a Facebook consumer to access an application directly by using their Facebook account and login credentials (username and password), rather than requiring the user to create a new set of credentials for the third-party application. Facebook Login then transmits information back to Facebook regarding what actions the consumers took and the information is then used to update their personal data profile. The Facebook platform also harmonizes third-party applications’ interfaces and integration with Facebook.

---

<sup>27</sup> *Id.*

60. The Facebook platform also includes an application program interface (“API”). The API specifies how software components interact. In practical terms, Facebook’s website is built upon proprietary source code. The API refers to the code that Facebook makes available to third-party developers in order for them to build applications for the Facebook website. The API allows for a third-party application to interact with the Facebook website and governs the extent to which it can access Facebook’s collection of consumer data.

61. Overall, the Facebook platform was designed to allow for the development of third-party applications that would seamlessly engage with Facebook consumers while at the same time allowing those applications access to Facebook’s vast collection of consumer data.

**C. The Cambridge Analytica Data Collection**

**i. The Harvesting of 70 Million Facebook Users’ Data**

62. In November 2013, Aleksandr Kogan, a researcher affiliated with Cambridge University, and his company GSR, launched a third-party application on the Facebook platform that identified itself as a personality study for research purposes. The application was called “thisisyourdigitallife” (“the App”) and ran on the Facebook platform for more than two years. The App presented itself to Facebook consumers as a personality quiz and generated a personality profile for consumers in exchange for downloading the App and granting access to some of the consumer’s personal data stored by Facebook.

63. The App was presented to Facebook as a research study regarding psychological traits. When the App launched, Facebook allowed third-party applications to be launched on the Facebook platform without affirmative review or approval by Facebook, meaning Facebook did not review the App before it was allowed on the Facebook platform, nor did it verify its claim that the information the App collected was for academic purposes.



64. At the time of the App's launch, Facebook policy allowed applications to request permission to access a Facebook consumer's personal data. Prior to installation, a Facebook consumer installing the App (an "App User") was shown an informational screen stating that the App would download some of their own personal data from Facebook, including their name, gender, birthdate, likes, and a list of Facebook friends.

65. To complete the installation, an App User clicked a Facebook Login icon on the information screen. The App was then installed through the Facebook Login service, using the App User's Facebook login credentials.

66. Upon installation, the App gathered the personal information of the App User from the Facebook vault of user data, including at least the App User's name, gender, birthday, likes, and list of Facebook friends.

67. Additionally, the App also expanded its reach and accessed the personal data of the App User's Facebook friends named on the list shared by the App User upon downloading the App. This data included at least the Facebook friend's name, gender, birthdate, current city, and likes. The vast majority of these Facebook friends never installed the App, never affirmatively consented to supplying the App with their data, and never knew the App had collected their data.

68. In early 2014, Facebook introduced changes to the Facebook platform that (i) limited the data that third-party applications could access, including data regarding the installing consumer's friends, and (ii) instituted a review and approval process (App Review) for applications that sought to access data beyond what the updated Facebook platform would allow. In May 2014, Kogan applied to App Review to request access to consumer data beyond what the updated Facebook platform would allow. In only a matter of days, Facebook rejected Kogan's application on the basis that he was seeking information beyond the App's stated research

purposes. Nevertheless, the App was still permitted to access consumer data beyond what the updated Facebook platform allowed through at least May 2015, due to a grace period Facebook granted existing applications following its update to the Facebook platform. This grace period was not absolute, and Facebook made numerous exceptions for other applications.

69. During the time that the App ran on the Facebook platform, approximately 290,000 Facebook consumers in the United States installed the App, including thousands of consumers in New Mexico. Because the App was improperly allowed to harvest the personal data of App Users as well as App Users' Facebook friends, approximately 70 million United States Facebook consumers had their information collected by the App, including nearly 350,000 residents in New Mexico.<sup>28</sup>

## **ii. Facebook Sells and Misuses Consumer Data**

70. In 2014, when the App was fully operational on the Facebook platform and harvesting consumers' data, Kogan entered into an agreement with Cambridge Analytica for the sale of data collected by the App. Cambridge Analytica was a political consulting firm based in London, England, that provided consulting services to candidates running for political office in the United States and abroad.

71. Kogan provided Cambridge Analytica with the harvested personal data and derivative data of the approximately 70 million United States Facebook consumers, including the information on the 350,000 New Mexico residents.<sup>29</sup> Kogan received over \$800,000 from Cambridge Analytica in exchange for this data.

---

<sup>28</sup> State-by-State Breakdown, *supra* n.5.

<sup>29</sup> *Id.*

72. Cambridge Analytica used the data it acquired from Kogan to, among other things, target digital political advertising during the 2016 United States Presidential Election (the “2016 Election”). Cambridge Analytica received millions of dollars from multiple presidential candidate campaigns to provide digital advertising services during the 2016 Election.

73. During this time, Facebook had employees embedded within multiple presidential candidate campaigns who worked alongside employees from Cambridge Analytica. Facebook knew, or should have known, that these presidential candidate campaigns and Cambridge Analytica were using the Facebook consumer data harvested by Kogan throughout the 2016 Election.

**D. Facebook’s Failure in Oversight and Enforcement of Its Own Policies**

74. At all times relevant to this Complaint, Facebook knew that it informed users that it would keep their information safe and allow them to control who saw it, but elected not to follow its own representations to consumers.

75. By no later than December 11, 2015, Facebook was made aware that Kogan previously sold Facebook consumer data to Cambridge Analytica. At that time, Facebook also knew that the collection and sale of consumer data violated its Platform Policy. Rather than investigate the sale further and recollect the data or oversee its destruction, Facebook accepted Kogan’s excuse that the data was being used for “research purposes,” and did nothing further to provide security for its users.<sup>30</sup>

---

<sup>30</sup> Chloe Aiello, *Developer behind the app at the center of data scandal disputes Facebook’s story*, CNBC (Mar. 21, 2018), available at <https://www.cnbc.com/2018/03/21/aleksander-kogan-facebook-shouldve-known-how-app-data-was-being-used.html>.

76. Facebook's Platform Policy, which governed its relationship with third-party application developers throughout the App's operation on the Facebook platform, expressly prohibited the transfer and sale of consumer data accessed from Facebook. However, Facebook failed to review or enforce its Platform Policy. Indeed, the App itself contained terms that directly contradicted the Platform Policy, expressly stating that collected data could be used for commercial purposes. Nevertheless, Facebook did not review this language, or if it did, Facebook did not take any action against the App and instead permitted it to harvest and sell Facebook consumer data without oversight or consumer permission.

77. The Platform Policy also permitted Facebook to audit any applications on the Facebook platform and to take enforcement measures as necessary if it suspected that an application was violating the Platform Policy. In addition, the Platform Policy expressly provided several methods by which Facebook could enforce compliance with the Platform Policy if an application was found to not be in compliance. These audit provisions were largely unenforced.

78. In late December 2015, Facebook terminated the App's access to the Facebook platform. Nevertheless, Facebook did not ban, suspend, or limit the privileges of Kogan, Cambridge Analytica, or any of their affiliates, with respect to their access to the Facebook website or the Facebook platform. Nor did Facebook conduct an audit of Kogan, Cambridge Analytica, or any of their affiliates, or take any other enforcement or remedial action to determine the status of the Facebook consumer data that was harvested by the App, including whether the data had been deleted and protected from further use and sharing.

79. Instead, Facebook simply requested that Kogan and Cambridge Analytica delete all data that they received through the Facebook platform. Rather than following up to ensure the data was removed from Kogan and Cambridge Analytica's files and databases, Facebook simply

accepted their word that they had done so. Facebook took no additional steps to determine whether the harvested data was, in fact, accounted for and destroyed. Facebook waited until August 2016 to send a letter to Cambridge Analytica requesting that the data that was illegally obtained be immediately destroyed. In actuality, the data was not destroyed. It continued to be held and used by Cambridge Analytica through the 2016 Election and beyond. Facebook knew, or should have known, that the data was not destroyed because, among other sources, its employees were embedded in presidential candidate campaigns during the 2016 Election, working alongside Cambridge Analytica employees and should have reported the use of the data to Facebook.

80. Facebook did eventually require written certifications from both entities promising that the harvested data was accounted for and destroyed. Facebook did not receive these written certifications from Kogan until June 2016 and did not receive a certification from Cambridge Analytica until April 2017.

81. Facebook declares to consumers that “Your trust is important to us” and suggests that it does not share personal information about users without permission or prior to giving notice, as part of its “Data Use Policy.” Facebook violated its own internal policies by not alerting consumers of the potential malevolent acquisition of their personal data.

82. In April 2018, years after the data was improperly harvested, Facebook finally disclosed to its consumers that their personal information may have been harvested and sold to Cambridge Analytica.

83. Facebook had the opportunity to disclose the sale of Facebook consumer data to Cambridge Analytica in 2015 or 2016. Had Facebook done so, it would have provided consumers with timely, material information about their use of Facebook. Had Facebook disclosed that consumers’ data was sold to a political consulting firm and was being used to target political

advertising for the 2016 Election, the disclosure would have influenced Facebook consumers, including consumers in New Mexico, to be more cautious in using Facebook. Among other actions, consumers may have opted to share less information on Facebook or deactivate their Facebook accounts altogether. Rather than make the required disclosures, Facebook instead profited from Kogan's and Cambridge Analytica's misuse of this harvested consumer data by selling millions of dollars of advertising space to Cambridge Analytica and presidential candidate campaigns during the 2016 Election.

84. Facebook knew, or should have known, of other third-party applications that similarly violated its Platform Policy by selling or improperly using consumer data. Facebook also failed to take reasonable measures to enforce its Platform Policy in connection with other third-party applications and failed to disclose to users when their data was sold or otherwise used in a manner inconsistent with Facebook's policies.

**E. Facebook's Statements and Practices Regarding Third-Party Application Access to Consumer Data Were False and Misleading**

85. Facebook knew or should have known that it needed to implement protection strategies after a 2011 complaint was prepared by the FTC against Facebook for allowing third-party applications to access consumers' personal data, either directly or through a Facebook friend authorizing it.

86. In order to resolve the FTC complaint, Facebook entered into the November 29, 2011 FTC Consent Order, which provided that Facebook was required not to misrepresent information pertaining to "the extent to which [Facebook] makes or has made covered information accessible to third parties," and "the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides. . . ." The Consent Order raised the level of

scrutiny placed on Facebook regarding its data security practices and implemented restrictions on providing personal data without a user's "affirmative express consent." *See* FTC Consent Order.

87. Facebook also outwardly represents its brand as one that takes data security seriously. But Facebook falsely represents to consumers that they have the ability to exercise a heightened level of control regarding their personal information. Users are told that they can customize who can see certain posts, add them as a friend, and are constantly reminded of security and privacy via images of padlocks on various settings pages and posts. In reality, Facebook promotes a false sense of safety for its users, as their information was constantly accessible to third-party applications and their developers.

88. Facebook made some disclosures about third-party application access to consumer data, but these disclosures were ambiguous, misleading, and deceptive. These disclosures are primarily contained in two lengthy documents, a Terms of Service and Data Policy, that consumers are required to agree to in order to create a Facebook account. These documents together set out Facebook's general terms of use, and contain statements regarding third-party applications' abilities to access a consumer's data. However, as shown by Facebook's actions (and inactions) in connection with third parties, including the App and Cambridge Analytica, the representations made in these documents were misleading and deceptive.

89. For the duration of the App's launch and operation on the Facebook platform, Facebook's Terms of Service represented that Facebook required applications to respect all Facebook consumers' privacy. This representation, taken with Facebook's public statements that it would protect consumers' private information and its representations in the Platform Policy that it had the ability to audit third-party applications and take enforcement measures against those

applications, falsely conveyed to consumers that Facebook had implemented and maintained reasonable oversight and safeguards to protect consumers' privacy.

90. These representations were misleading and deceptive, as demonstrated by Facebook's lack of oversight and enforcement relating to third parties, such as the App. For example, Facebook did not conduct meaningful oversight or enforcement of the App at several relevant times when it knew, or should have known, that the App was operating in violation of Facebook's policies, including: (i) when the App was first launched on the Facebook platform; (ii) after Facebook became aware, through its receipt and rejection of Kogan's application through App Review, that the App was seeking consumer data to be used beyond the App's stated "research purpose"; and (iii) after it learned that data collected by the App had been sold to Cambridge Analytica.

91. In addition, Facebook's Data Policy also contained misrepresentations about third-party applications' access to Facebook consumer data. From at least November 15, 2013, to at least January 30, 2015, the Data Policy provided that if an application asks permission from someone else to access a user's information, the application is permitted to then use that information only in connection with the person that gave permission, and no one else. This representation was deceptive and misleading, as demonstrated by Kogan's use of the App to harvest consumer data, and then sell it to Cambridge Analytica. Facebook failed to implement and maintain reasonable oversight of applications operating on the Facebook platform to safeguard consumers' private data, and it knew or should have known that it did not have necessary measures in place to control how applications used and/or shared data.

92. Facebook also misled its consumers generally about third-party applications' access to user data. Facebook publicly represented that consumers controlled how their data is



shared on the Facebook website. But as shown by the App, third-party applications that a Facebook consumer had never downloaded could still access their information through a Facebook friend who downloaded the App. The Facebook platform thus afforded third parties an end-run to access consumer data, which third-party applications exploited. Facebook failed to disclose, or failed to adequately disclose, this material fact to its consumers in a timely manner.

93. Adding to Facebook's deception of consumers is the fact that consumers could not restrict third-party application access to their data through Facebook's Privacy Settings. A consumer would expect to have the ability to control how their data is shared, given the pages of security questions they are required to review. Instead, Facebook allocated privacy settings related to applications to a separate location under a separate Application Settings tab accessible to consumers.

94. When Cambridge Analytica was able to purchase access to this repository of data for just millions of dollars, employees at the company were then able to enact their plan to "harvest the Facebook profiles of millions of people in the U.S." in order to build personal profiles of the users for targeted advertising and psychological persuasion.<sup>31</sup> These personal profiles were in turn leveraged by political strategists.<sup>32</sup> This single incident serves as a prime example of the dangers Facebook users, as individuals and the nation as a whole, were subjected to due to Facebook's nonchalant approach to data security measures.

95. As previously mentioned, consumers are led to believe that their data is secured through Privacy Settings, where consumers control how their Facebook information is shared with

---

<sup>31</sup> Carole Cadwalladr, *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, The Guardian (Mar. 18, 2018), available at <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.

<sup>32</sup> *Id.*

other Facebook users. For example, consumers can control the types of other Facebook users that can view their account information. This can be adjusted to allow for sharing to all Facebook consumers (most expansive), only Facebook friends (the more limited default), and a customized list of Facebook friends (the most restrictive).

96. By contrast, through Application Settings, consumers control how their Facebook information is shared with third-party applications. But these controls were highly misleading: for example, from at least November 2013 through at least April 2014, even if a consumer restricted access to his or her information to only Facebook friends through the Privacy Settings, the information could still be accessible by any application that the consumer's friends downloaded. This loophole was well known to application developers, including Kogan and Cambridge Analytica and their partners.

97. In sum, Facebook's representations and omissions regarding consumer privacy, in connection with applications' access to private information, were misleading and deceptive in a number of ways:

- a. Facebook's lack of adequate disclosures and multi-tiered privacy options failed to disclose to consumers how their information was shared with applications, as opposed to other Facebook users.
- b. Facebook failed to tell consumers for over two years that their personal information was improperly harvested and sold by Kogan to Cambridge Analytica in violation of Facebook's policies.
- c. Facebook's representations to consumers that it would protect the privacy of consumers' personal information, when, in fact, it did not implement or maintain reasonable privacy safeguards and failed to take reasonable measures in response

to the harvesting and use of data by Cambridge Analytica, were misrepresentations of material facts.

- d. Facebook's representations to consumers that it requires applications and third-party developers to respect the privacy of consumers' personal information and data, when, in fact, it did not implement or maintain reasonable oversight of third-party applications or enforcement mechanisms for its active security policies, are also misrepresentations of material facts that continue to mislead consumers.
- e. Facebook's representations to consumers that consumers' agreements with third-party applications will control how those applications use consumer data, when, in fact, applications were able to collect and use consumer data without regard to those agreements, are misrepresentations of material facts that continue to mislead consumers.
- f. Facebook's failure to adequately inform consumers that their personal information may be shared with third-party applications without their knowledge or affirmative consent is an omission that misled consumers.
- g. Facebook's failure to explain to consumers how to control the way by which information is shared with third-party applications and how to change privacy settings with respect to third-party applications, and its representations that consumers can control how their information is shared, constitute omissions of material facts that are misleading to consumers.

**F. Facebook's Misleading Statements and Practices Regarding Partner Company Access to Consumer Data Provide Another Example of Misuse of Consumer Data**

98. Facebook's failure to follow its own promises was pervasive, extending beyond failing to restrict private information.

99. In addition to third-party applications, Facebook also improperly granted partner companies, many of whom were mobile device makers, access to Facebook's collection of consumer data.

100. Today, most consumers accessing Facebook through their mobile devices do so through the Facebook mobile application on their smartphone or tablets. Prior to the widespread use of the Facebook mobile application on personal cell phones, however, Facebook entered into integration partnerships with various device makers to develop Facebook applications specific to their devices.

101. Through these arrangements, applications were permitted access to Facebook consumer data, including the data of those Facebook consumers who downloaded the application and the data of their Facebook friends. Consumers had little or no control over whether to permit the sharing of their information to these companies.

102. Facebook's sharing of user data was uncontrolled—indeed, it revealed in July 2020 that it shared user data with thousands of developers even after access should have expired.<sup>33</sup>

103. Facebook entered into at least 52 integration partnerships with other companies. Facebook also extended similar access to Facebook consumer data to other partner companies.

104. Facebook's failure to inform consumers that it permitted certain companies to override Facebook consumers' privacy settings and access their information without their knowledge or consent constitute omissions of material facts that misled consumers.

---

<sup>33</sup> Queenie Wong, *Facebook shared user data with developers after access should have expired*, C|Net (July 1, 2020), <https://www.cnet.com/news/facebook-shared-user-data-with-developers-after-access-should-have-expired/>.

105. Facebook’s representations that consumers can control how their information is shared, when, in fact, certain partner companies were able to override those controls, constitute misrepresentations of material facts that misled consumers.

**G. Facebook’s Refusal to Police Its Own Site Creates Additional Cybersecurity and Privacy Risks**

106. The multiple warning signs concerning Facebook’s problems with keeping user information private also alerted Facebook to the additional problems flouting its own privacy policies would cause: the spread of misinformation, viral propaganda, and “inspir[ing] deadly campaigns of hate around the globe.”<sup>34</sup>

107. Facebook’s violations of its own privacy policies and the spread of harmful misinformation go hand-in-hand. Transparency tools developed by Facebook to prevent the spread of misinformation have been ineffective, allowing wrongdoers to exploit scraped user information to target individuals with problematic ads and spread propaganda and hoaxes.<sup>35</sup> Facebook’s algorithm, itself, exacerbates the problem, providing consumers with more and more misinformation with every “like.”

108. Importantly, Facebook’s algorithms are Facebook’s own creation. These algorithms have nothing to do with posts made by third-parties on Facebook’s platform. Indeed,

---

<sup>34</sup> Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg, and Jack Nicas, *Delay, Deny and Deflect: How Facebook’s Leaders Fought Through Crisis*, The New York Times (Nov. 14, 2018), <https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html>.

<sup>35</sup> See, e.g., Alfred Ng, *Senators demand Zuckerberg fix Facebook’s ad transparency tool*, C|Net (Nov. 2, 2018), <https://www.cnet.com/news/senators-demand-zuckerberg-fix-facebooks-ad-transparency-tool/>; Alfred Ng, Joan E. Solsman, *Facebook’s InfoWars, fake news, Alex Jones problems aren’t going away*, C|Net (July 18, 2018), <https://www.cnet.com/news/facebooks-infowars-fake-news-alex-jones-problems-arent-going-away/>.

these algorithms form the very backbone of Facebook's platform, and such algorithms are regarded as some of the most valuable intellectual property on Earth.<sup>36</sup>

109. Facebook's algorithms are designed to ingest information about consumers and then improperly use that information to deliver consumers content selected specifically to keep consumers on the site, even if such information is harmful, misleading, or outright false.

110. For example, Facebook likes, comments, and shares of articles from news outlets that regularly publish provably false content and misleading, unsubstantiated claims roughly tripled from the third quarter of 2016 to the third quarter of 2020.<sup>37</sup> The growth rate of likes, shares, and comments of content from manipulators and false content producers exceeded the interactions that users had with legitimate journalistic outlets such as Reuters, Associated Press, and Bloomberg.<sup>38</sup> This explosion was made possible by Facebook's misuse of consumer information via Facebook's own proprietary algorithms.

111. Facebook can address these issues if it desires, and did so temporarily in the run-up to the 2020 presidential election by tweaking its algorithms to elevate posts from trusted news sources over hyper-partisan, less trustworthy sources that amplified falsehoods.<sup>39</sup> But because Facebook relies on viral content to bring in users, who it can then show ads to, tamping down

---

<sup>36</sup> See, e.g. Martin, Nicole, *Facebook files algorithm patent to predict who you live with*, Forbes (Nov. 20, 2018), available at <https://www.forbes.com/sites/nicolemartin1/2018/11/20/facebook-files-algorithm-patent-to-predict-who-you-live-with/?sh=37fc52635449>.

<sup>37</sup> Davey Alba, *On Facebook, Misinformation Is More Popular Now Than in 2016*, The New York Times (Oct. 12, 2020), <https://www.nytimes.com/2020/10/12/technology/on-facebook-misinformation-is-more-popular-now-than-in-2016.html>.

<sup>38</sup> *Id.*

<sup>39</sup> Eric Lutz, *WITH THE ELECTION OVER, FACEBOOK GETS BACK TO SPREADKING MISINFORMATION: Turns out what's good for the world is bad for Mark Zuckerberg's bottom line*, Vanity Fair (Dec. 17, 2020), <https://www.vanityfair.com/news/2020/12/with-the-election-over-facebook-gets-back-to-spreading-misinformation>.

misinformation runs against Facebook’s economic incentives.<sup>40</sup> In experiments Facebook conducted in November 2020, posts users regarded in surveys as “bad for the world” tended to have a greater reach, and algorithmic changes that reduced the visibility of those posts also reduced users’ engagement with the platform.<sup>41</sup> Accordingly, Facebook did away with the algorithm modification that prioritized credible news sources, once again deciding to misuse consumers’ information to deliver those consumers fake and hyper-partisan news because the ad-based business model favors it.

112. Facebook’s promise to protect sensitive user information does little to combat the spread of misinformation. As part of the platform’s “pivot to privacy” after the 2016 election, Facebook promoted “groups”—private pages for users with similar interests moderated by group moderators with little to no oversight from Facebook—as trusted spaces that create communities.<sup>42</sup> As Zuckerberg explained in a 2019 blog post, “Many people prefer the intimacy of communicating one-on-one or with just a few friends. People are more cautious of having a permanent record of what they’ve shared.”<sup>43</sup>

113. In groups, users share, spread and receive information directly to and from their closest contacts, whom they typically see as reliable sources.<sup>44</sup> But groups continue to be used for political information, partly due to the lack of transparency in the ownership, management and

---

<sup>40</sup> *Id.*

<sup>41</sup> *Id.* See also, Kevin Roose, Mike Isaac and Sheera Frenkel, *Facebook Struggles to Balance Civility and Growth: Employees and executives are battling over how to reduce misinformation and hate speech without hurting the company’s bottom line.*, The New York Times (Nov. 24, 2020), <https://www.nytimes.com/2020/11/24/technology/facebook-election-misinformation.html>.

<sup>42</sup> Nina Jankowicz and Cindy Otis, *Facebook Groups Are Destroying America*, Wired (June 17, 2020), <https://www.wired.com/story/facebook-groups-are-destroying-america/>.

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

membership of groups.<sup>45</sup> Groups provide a menu of potential targets organized by issue and even location; bad actors can create fake profiles or personas tailored to the interests of the audiences they intend to infiltrate, seeding their own content into a group, and/or repurposing the group's content for use on other platforms.<sup>46</sup> Facebook then algorithmically suggests additional groups and Related Pages based on groups users' recent engagement and activity, and the cycle of disinformation continues.<sup>47</sup>

114. Moreover, Facebook's news feed algorithm mines users' data to cater content to users' already-held beliefs. The algorithm first scans and collects everything posted in the past week by each of a user's friends, everyone the user follows, each group the user belongs to, and every Facebook page the user has liked, then ranks them all in order of how likely the user is to find each post worthwhile.<sup>48</sup> The algorithm doesn't only predict whether the user will actually like the post based on past behavior, it also predicts whether the user will click, comment, share, hide, or mark the post as spam, creating a single relevancy score that is particular to the user and that post.<sup>49</sup> Every possible post receives a relevancy score, which the sorting algorithm puts in the order

---

<sup>45</sup> *Id.*

<sup>46</sup> *Id.* Users coordinating their activities across networks of groups and pages managed by a small handful of people boost false narratives. As an example, at least nine coordinated pages and two groups—with more than 3,000,000 likes and 71,000 members respectively—are set up to drive traffic to five “news” websites that promote hyper-partisan conspiracy theories. *Id.*

<sup>47</sup> *Id.* See also, ‘Facebook Groups Are Destroying America’: Researcher On Misinformation Spread Online, NPR, All Things Considered (June 22, 2020), <https://www.npr.org/2020/06/22/881826881/facebook-groups-are-destroying-america-researcher-on-misinformation-spread-onlin>.

<sup>48</sup> Will Oremus, *Who Controls Your Facebook Feed*, Slate (Jan. 3, 2016), [http://www.slate.com/articles/technology/cover\\_story/2016/01/how\\_facebook\\_s\\_news\\_feed\\_algorithm\\_works.html](http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html).

<sup>49</sup> *Id.*



that the user sees the posts on the screen.<sup>50</sup> The post at the top of a user’s feed, therefore, has been chosen over thousands of others as the most likely to make the user interact with the platform.<sup>51</sup> This creates “filter bubbles” in which users see only the content they like and agree with while Facebook hides dissenting points of view, and in effect, results in ideological bubbles where hyperpartisan news and misinformation run rampant.<sup>52</sup>

115. The proliferation of “groups” and the use of algorithmic targeting in the lead-up to the November 2020 election and thereafter allowed misinformation to spread at a breakneck pace. The spread of lies reached a boiling point on January 6, 2021, when violent insurrectionists acted upon conspiracy theories to storm the United States Capitol, attempting to interrupt the peaceful transfer of power during a joint session of Congress.

116. Facebook had ample warning to stop the spread of misinformation leading up to the congressional joint session. Rioters had openly discussed what they aimed to do in Washington on a Facebook page called Red-State Secession *for weeks*. The page had asked its roughly 8,000 followers to share addresses of perceived “enemies” in the citadel of democracy, including the home addresses of federal judges, members of Congress, and prominent progressive politicians.<sup>53</sup> Comments left on the page often featured photos of guns and ammunition, along with emojis suggesting that members of the group were planning for violence. One post said people should be

---

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> Selena Larson, *Facebook Shows you what you want to see post-election*, CNN Business (Nov. 9, 2016), <https://money.cnn.com/2016/11/09/technology/filter-bubbles-facebook-election/index.html>.

<sup>53</sup> Kate Conger, Mike Isaac and Sheera Frenkel, *Twitter and Facebook Lock Trump’s Accounts After Violence on Capitol Hill*, The New York Times (Jan. 6, 2021), <https://www.nytimes.com/2021/01/06/technology/capitol-twitter-facebook-trump.html>.

“prepared to use force to defend civilization.”<sup>54</sup> Several comments below the post showed photos of assault rifles, ammunition and other weapons. In the comments, people referred to “occupying” the Capitol, and taking action to force Congress to overturn the results of the elections.<sup>55</sup> Facebook took action after weeks of negligence—finally removing the Red-State Secession page on the morning of the January 6 siege.<sup>56</sup>

117. Facebook acted—but only after five people were killed in the insurrection. Facebook finally suspended Mr. Trump’s Facebook and Instagram accounts indefinitely after the Capitol siege.<sup>57</sup> Facebook also said it would remove other content, including so-called “Stop the Steal” groups (which had spread misinformation that the election was “stolen”),<sup>58</sup> as well ban “militarized social movements” and the “violence-inducing conspiracy theory QAnon,” while continuing to enforce its ban on hate groups including the Proud Boys.<sup>59</sup> Facebook also stated it would search for and remove content that praised the storming of the U.S. Capitol, calls to bring weapons to locations across the U.S., including protests, incitement or encouragement of the events

---

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> Guy Rosen and Monika Bickert, *Facebook: Our Response to the Violence in Washington*, Facebook (Jan. 6, 2021), <https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/>. See also Mike Isaac and Kate Conger, *Facebook Bars Trump Through End of His Term*, The New York Times (Jan. 7, 2021, updated Jan. 8, 2021), <https://www.nytimes.com/2021/01/07/technology/facebook-trump-ban.html>. See also, Mike Isaac and Kate Conger, *Facebook banned Trump from its platforms for the rest of his term for inciting violence*, The New York Times (Jan. 7, 2020), <https://www.nytimes.com/2021/01/07/us/politics/facebook-banned-trump-from-its-platforms-for-the-rest-of-his-term-for-inciting-violence.html>.

<sup>58</sup> Stuart A. Thompson and Charlie Warzel, *They Used to Post Selfies. Now They’re Trying to Reverse the Election: Right-wing influencers embraced extremist views, and Facebook rewarded them*, The New York Times (Jan. 14, 2021), <https://www.nytimes.com/2021/01/14/opinion/facebook-far-right.html?referringSource=articleShare>.

<sup>59</sup> Guy Rosen and Monika Bickert, *Facebook: Our Response to the Violence in Washington*, Facebook (Jan. 6, 2021), <https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/>.

at the Capitol, calls for protests that violated D.C. curfew, and attempts to restage the violence in coming days.<sup>60</sup> Removing Mr. Trump and certain groups from its platform supposedly limits dangerous content from spreading further, but the ideas and sentiments that those removals would supposedly quell still blanket the platform.<sup>61</sup> Moreover, groups that have been removed are reappearing as “different” groups, sometimes under nearly identical names.<sup>62</sup>

118. These recent removal efforts by Facebook to address discord and violence—which Facebook has not only long abided and even encouraged through its algorithms, but also has profited immensely from—is much too little, too late. Facebook has played a long-running, significant role in the spread of misinformation and the fomentation of extremism—on its platform and beyond—all for the single purpose of prioritizing profits over people, culminating with the violent deaths of five people,<sup>63</sup> with dozens injured.<sup>64</sup>

119. Facebook’s swift removal of myriad Facebook posts leading up to the events of January 6, 2021 (including Facebook public posts and Facebook Live video streaming of the siege itself),<sup>65</sup> as well as the revocation of numerous accounts (including Mr. Trump’s), demonstrate the swift ability of Facebook to enforce its own content policies. Its social media dominance and self-

---

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> Jack Healy, *These Are the 5 People Who Died in the Capitol Riot*, The New York Times (Jan. 11, 2021), <https://www.nytimes.com/2021/01/11/us/who-died-in-capitol-building-attack.html>.

<sup>64</sup> Sara Morrison, *the Capitol rioters put themselves all over social media. Now they’re getting arrested.*, Vox (Jan. 12, 2021), <https://www.vox.com/recode/22218963/capitol-photos-legal-charges-fbi-police-facebook-twitter>. See also Stuart A. Thompson and Charlie Warzel, *They Used to Post Selfies. Now They’re Trying to Reverse the Election: Right-wing influencers embraced extremist views, and Facebook rewarded them*, The New York Times (Jan. 14, 2021), <https://www.nytimes.com/2021/01/14/opinion/facebook-far-right.html?referringSource=articleShare>.

<sup>65</sup> Sara Morrison, *the Capitol rioters put themselves all over social media. Now they’re getting arrested.*, Vox (Jan. 12, 2021), <https://www.vox.com/recode/22218963/capitol-photos-legal-charges-fbi-police-facebook-twitter>.

governance has never been more obvious than in the wake of a national tragedy. Facebook clearly has the power to control its platform, and yet has consistently and repeatedly failed to act, with dire consequences.

120. Facebook's ability to enforce its own policies also underscore Facebook's myriad failures to prevent private information from being used and weaponized. Consumers placed trust in Facebook to keep their information secure. Instead, Facebook allowed unauthorized parties to access that information, and use it to spread false and misleading information back to Facebook's users.

## **VI. CLAIMS AND VIOLATIONS ALLEGED**

### **VIOLATION OF THE NEW MEXICO UNFAIR PRACTICES ACT**

121. The State incorporates the allegations of Paragraphs 1-120 of this Complaint into this claim.

122. The Unfair Practices Act, NMSA 1978, Sections 57-12-1 to -26, is legislation that prohibits the economic exploitation of consumers in the State of New Mexico by, among other means, unfair, false, deceptive, or misleading advertising or the conduct of business in an unfair manner.

123. Facebook is a "person" pursuant to Section 57-12-2(A).

124. Facebook's Services are "services" under the Unfair Practices Act.

125. According to Section 57-12-2(D) an "unfair or deceptive trade practice" means "an act specifically declared unlawful pursuant to the Unfair Practices Act, a false or misleading oral or written statement, visual description or other representation of any kind knowingly made in connection with the sale, lease, rental or loan of goods or services or in the extension of credit or in the collection of debts by a person in the regular course of his trade or commerce, which may, tends to or does deceive or mislead any person and includes:

(5) representing that. . . services have. . . characteristics. . . [or] benefits. . . that they do not have. . .;

. . .

(14) using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if doing so deceives or tends to deceive;

. . .

or

(17) failure to deliver the quality. . . of. . . services contracted for. . .

126. According to Section 57-12-2(E), an “unconscionable trade practice” means an “act or practice in connection with the sale, lease, rental or loan, or in connection with the offering for sale, lease, rental or loan, of any goods or services. . .” which:

(1) takes advantage of the lack of knowledge, ability, experience or capacity of a person to a grossly unfair degree; or

(2) results in a gross disparity between the value received by a person and the price paid.

127. Pursuant to Section 57-12-3, “[u]nfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce are unlawful.”

128. Defendant Facebook repeatedly and continuously made unfair, deceptive, false, or misleading statements and omissions regarding the security of consumers’ data from the moment Facebook partnered with third-party applications that it gave elevated permissions to alter consumers’ privacy settings.

129. Facebook’s omissions and misrepresentations prevented consumers from understanding how Facebook would use their data, share their data with developers, and ignore users’ requests to keep their information private. Facebook’s acts were unconscionable because it took advantage of the lack of knowledge consumers had about its actual practices, including with

its algorithms, creating a gross disparity between what consumers bargained for by sharing their information, versus the services they received.

130. Facebook's representations to consumers, both express and implied, that it will protect the privacy of consumers' personal information, that it requires applications and third-party developers to respect the privacy of consumers' personal information, and that consumers' agreement with third-party applications will control how those applications use consumer data, are misrepresentations concerning material facts that mislead and have misled consumers, and are unfair and deceptive trade practices that violate the UPA.

131. Facebook's failure to disclose, or failure to adequately disclose, to consumers that their personal information may be shared with third-party applications without their knowledge or affirmative consent is a material fact, the omission of which misled consumers and are unfair and deceptive trade practices that violate the New Mexico Unfair Trade Practices Act.

132. Facebook's failure to disclose, or failure to adequately disclose, to consumers that its algorithms would use consumers' own data to then target those consumers with misinformation and conspiracy theories based upon their prior exposure to such information is a material fact, the omission of which misled consumers and are unfair and deceptive trade practices that violate the New Mexico Unfair Trade Practices Act.

133. Further, Facebook's misuse of consumers' data to systematically mislead consumers into believing that sources of information appearing on their news feeds and in their groups are as trusted or reliable as consumers' self-selected sources of information constitutes an unconscionable trade practice that takes advantage of the lack of knowledge consumers have about Facebook's actual practices.

134. Facebook’s failure to disclose, or failure to adequately disclose, to consumers that their personal information was improperly harvested and used by third-party applications and others in violation of Facebook’s policies is a material fact, the omission of which mislead and have misled consumers, and are unfair and deceptive trade practices that violate the New Mexico Unfair Trade Practices Act.

135. Facebook’s failure to explain to consumers how to control the way by which information is shared with third-party applications and how to change privacy settings with respect to applications, as well as its representations to consumers, both express and implied, that it will protect the privacy of consumers’ personal information, that it requires applications and third-party developers to respect the privacy of consumers’ personal information, and that consumers’ agreement with third-party applications will control how those applications use consumer data, constitute omissions of material facts that misled consumers and are unfair, deceptive, and unconscionable trade practices that violate the UPA.

136. Facebook made these material omissions and misrepresentations to consumers via its uniform policies—which purported to provide consumers with assurances that their most sensitive and “private” information would be protected.

137. Facebook also made these material omissions and misrepresentations to consumers without adequately disclosing to them that such misinformation is pervasive across its platform.

138. Facebook’s failure to disclose to consumers that it permitted certain companies to override Facebook consumers’ privacy settings and access their information without their knowledge or consent are material facts, the omission of which misled consumers and are unfair and deceptive trade practices that violate the UPA.

## **VII. REQUEST FOR RELIEF**

WHEREFORE, Plaintiff, the State of New Mexico, respectfully requests that the Court enter a judgment in its favor and grant relief against Defendant Facebook, Inc. as follows:

- (a) Awarding the maximum amount of statutory penalties available under Section 57-12-11, for each of Facebook's violation of New Mexico's Unfair Trade Practices Act;
- (b) Ordering Facebook to disgorge all profits that it illegally obtained by and through its illegal conduct, and used to further fund or promote the illegal conduct or that constituted capital available for that purpose;
- (c) Awarding Plaintiff its attorneys' fees and litigation costs; and,
- (d) Awarding such other relief as may be available and appropriate under the law or in equity.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK



### **VIII. JURY DEMAND**

Plaintiff demands a trial by jury for all claims upon which a jury trial is available.

Dated: January 21, 2021

Respectfully submitted,

**Hector H. Balderas**  
**ATTORNEY GENERAL**

/s/ P. Cholla Khoury

P. Cholla Khoury  
Assistant Attorney General  
408 Galisteo Street  
Villagra Building  
Santa Fe, New Mexico 87501  
Tel: (505) 490-4052  
Email: ckhoury@nmag.gov

*By special commission and pro hac vice  
motions to be filed:*

Adam J. Levitt  
Amy E. Keller  
Daniel R. Ferri  
Mary McKenna  
**DICELLO LEVITT GUTZLER LLC**  
Ten North Dearborn Street, Sixth Floor  
Chicago, Illinois 60602  
Tel: (312) 214-7900  
Fax: (312) 253-1443  
Email: alevitt@dicellolevitt.com  
akeller@dicellolevitt.com  
dferri@dicellolevitt.com  
mmckenna@dicellolevitt.com

Mark A. DiCello  
Justin Hawal  
**DICELLO LEVITT GUTZLER LLC**  
Western Reserve Law Building  
7556 Mentor Avenue  
Mentor, Ohio 44060  
Tel: (440) 953-8888

Fax: (440) 524-1662

Email: [madicello@dicellolevitt.com](mailto:madicello@dicellolevitt.com)

[jhawal@dicellolevitt.com](mailto:jhawal@dicellolevitt.com)

# EXHIBIT B



DICELLO LEVITT

TEN NORTH DEARBORN STREET SIXTH FLOOR CHICAGO, ILLINOIS 60602

ADAM J. LEVITT  
ALEVITT@DICELLOLEVITT.COM  
312.214.7900

January 13, 2023

**BY .PDF EMAIL (RFalconer@gibsondunn.com)**

Mr. Russ Falconer  
Gibson, Dunn & Crutcher LLP  
2001 Ross Avenue, Suite 2100  
Dallas, Texas 75201

**Re: *State of New Mexico ex rel. Balderas v. Facebook, Inc.*  
No. D-101-cv-2021-00132 (Santa Fe Cty.)**

Dear Russ,

We write on behalf of the New Mexico Attorney General's Office concerning Meta's proposed settlement of the multidistrict litigation in *In re Facebook, Inc. Consumer Privacy User Profile Litigation*, 18-md-02843-VC (N.D. Cal.) (the "MDL"). The New Mexico Attorney General's Office has reviewed the settlement agreement made public on December 22, 2022 at ECF No. 1096-2 (the "Settlement Agreement"). We note that the terms of the Settlement Agreement release certain claims of "Settlement Class Members," defined as "all Facebook users in the United States during the Class Period." Given that the claims asserted by the State of New Mexico in *State of New Mexico, ex rel. Hector Balderas, Attorney General v. Facebook, Inc.*, No. D-101-CV-2021-00132 (Santa Fe Cty.) (the "State's Action") are not brought by, or even on behalf of, any Facebook users, we write to confirm the State's understanding that the Settlement Agreement does not release any of the State's claims.<sup>1</sup>

---

<sup>1</sup> The foregoing does not constitute a comprehensive analysis of the Settlement Agreement. There may well be additional independent reasons why the Settlement Agreement language does not release the State's claims, all of which are expressly preserved and not waived. Moreover, the Attorney General intends to opt out of the settlement in an abundance of caution, which shall not be construed as an admission that any claims brought by the Attorney General would otherwise be subject to the release in the Settlement Agreement.

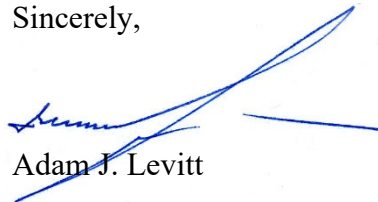
Mr. Russ Falconer  
January 13, 2023

We also note that Meta had an obligation pursuant to the Northern District of California's Procedural Guidance for Class Action Settlements to, within one day of the filing of the preliminary approval motion, notify "any plaintiffs with pending litigation ... asserting claims on a representative (e.g., class, collective, PAGA, etc.) basis that defendants believe may be released by virtue of the settlement." The New Mexico Attorney General received no such notification from Meta, which is consistent with our understanding that the Settlement Agreement neither impacts nor releases, in any manner, the claims brought against Meta by the State of New Mexico in the State's Action.

Please confirm, in writing and no later than January 20, 2023, that Meta agrees unequivocally that the Settlement Agreement does not release or otherwise impact any of the State's claims raised in the State's Action, and that Meta will not raise any arguments in any future proceeding to the contrary. Failure to do so will require that we intervene and/or object in the MDL proceedings, in order to protect and preserve the claims asserted in the State's Action.

Thank you.

Sincerely,



Adam J. Levitt

# EXHIBIT C

**From:** Falconer, Russ <RFalconer@gibsondunn.com>

**Sent:** Tuesday, February 28, 2023 8:01 AM

**To:** Adam J. Levitt <alevitt@dicellolevitt.com>; Corban Rhodes <crhodes@dicellolevitt.com>

**Subject:** RE: Facebook NMAG -- State of New Mexico's letter to Meta, re NMAG v. Facebook -- 011323.pdf (00915773.PDF;1).PDF

Corban and Adam:

You've asked for Facebook's position on whether the release in the proposed MDL settlement will have any effect on the State of New Mexico's litigation. To be clear, Facebook does not intend to ask the MDL court to issue a ruling on this issue, or to enjoin the State's case. That issue should be decided, if necessary, on an appropriate motion by the court in which any potentially affected action is pending, and only if and after a final settlement is approved. Facebook reserves its rights to raise this issue to the New Mexico court at an appropriate time.

To the extent that the State of New Mexico seeks to recover in *parens patriae* or otherwise seeks restitution on behalf of New Mexico consumers, Facebook anticipates taking the position that the release in the proposed MDL settlement (if granted final approval by the MDL court) operates to release that claim. To the extent the State seeks to recover other relief (e.g., civil penalties), Facebook reserves all rights.

Thanks,

Russ

**Russ Falconer**

**GIBSON DUNN**

Gibson, Dunn & Crutcher LLP  
2001 Ross Avenue Suite 2100, Dallas, TX 75201  
Tel 214.698.3170 • Cell 214.803.5487  
[RFalconer@gibsondunn.com](mailto:RFalconer@gibsondunn.com) • [www.gibsondunn.com](http://www.gibsondunn.com)

---

This message may contain confidential and privileged information for the sole use of the intended recipient. Any review, disclosure, distribution by others or forwarding without express permission is strictly prohibited. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message.

Please see our website at <https://www.gibsondunn.com/> for information regarding the firm and/or our privacy policy.

---